

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE APPLICATION OF  
THE UNITED STATES FOR:

AN ANTICIPATORY SEARCH WARRANT  
FOR THE RESIDENCE LOCATED AT: 715  
CLEAR RIDGE ROAD, ARTEMAS, PA 17211

Magistrate No. 3:20-123 MJ  
[UNDER SEAL]

INSTALLATION OF A GPS TRACKER IN A  
BOX WRAPPED IN BROWN TAPE,  
ADDRESSED TO "RIGGS VISER" WITH  
RETURN ADDRESSEE LISTED AS  
"MATSTORE"

Magistrate No. 3:20-124 MJ  
[UNDER SEAL]

INSTALLATION OF AN ELECTRONIC  
ALERTING DEVICE AS A PHYSICAL  
SURVEILLANCE AID

**AFFIDAVIT IN SUPPORT OF AN APPLICATION  
UNDER RULE 41 FOR A SEARCH AND SEIZURE WARRANT**

I, Brianna Maria Tetrault, having being duly sworn, depose and state as follows:

1. I, BRIANNA MARIA TETRAULT, am a Special Agent of Homeland Security Investigations (HSI) Immigration and Customs Enforcement (ICE), United States Department of Homeland Security. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States, who is empowered by law to conduct investigations of, and make arrests for, controlled substance offenses enumerated in Title 21, United States Code.

2. I am currently assigned to the HSI Pittsburgh Office of the Assistant Special Agent in Charge in the Contraband Smuggling Group and have been so employed since June 2010. As a Special Agent, I am authorized to conduct investigations of alleged violations of Immigration laws and Customs laws, including offenses involving the importation of prohibited

items, such as narcotics, under Titles 18, 19, and 21 of the United States Code. While being trained as a Special Agent of the HSI, your affiant has received basic training at the Federal Law Enforcement Training Center located in Glynco, Georgia. Your affiant has participated in a number of narcotics and money laundering investigations, which have resulted in the seizure of illegal drugs and evidence of drug violations, as well as the seizure of assets acquired with drug proceeds. Your affiant has conducted covert surveillance of suspected drug traffickers on numerous occasions, interviewed numerous individuals involved in the drug trafficking trade, participated in a Title III wiretap investigation, participated in the execution of numerous search and arrest warrants, assisted in the arrest of narcotics traffickers, and assisted in the seizure of controlled substances. Based upon the above experience, your affiant is familiar with the modus operandi of persons involved in illicit distribution of controlled substances, as well as the terminology used by persons involved in the illicit distribution of controlled substances. Your affiant is aware that persons involved in the illicit distribution of controlled substances routinely attempt to conceal their identities, as well as the location at which drug transactions take place.

3. I previously worked for the Pennsylvania Office of Attorney General, Bureau of Consumer Protection, from June 2006 to May 2010. As a Consumer Protection Agent, I investigated and enforced Pennsylvania Consumer Protection Laws. In 2006, I received a Bachelor's of Arts degree in Government and History from Arcadia University in Glenside, Pennsylvania.

4. The facts and information contained in this affidavit are based upon my personal participation in this investigation as well as information provided by other law enforcement officers involved in this investigation, specifically, but not limited to: Officers of the U.S. Customs and Border Protection Service (CBP), United States Postal Inspection Service (USPIS) and

Pennsylvania State Police. I make this affidavit in support of an application for a Search Warrant (anticipatory) for a residence located at 715 Clear Ridge Road, Artemas, PA 17211 (which is further described in attachment A), for the installation of a GPS Tracking Device, and for the installation of an Electronic Alerting Device.

5. As a result of my personal experience and my interactions and direct involvement with federal, state, and local agents/officers, I have become familiar with the various practices, tools, trends, paraphernalia, and related articles utilized by various traffickers in their efforts to import, possess, manufacture, and distribute controlled substances.

6. As a federal law enforcement officer, I am authorized to investigate violations of laws of the United States, including the crimes outlined herein, and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

This affidavit is made in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for the issuance of anticipatory warrant to search for and seize evidence, instrumentalities, contraband, and fruits of violations of Title 18, United States Code 545 (Smuggling), Title 21, United States Code, Sections 841(a)(1), 843(a)(6), and 846 (Conspiracy), at **715 Clear Ridge Road, Artemas, PA 17211** (the “**TARGET RESIDENCE**”), as further described in Attachment A, which is appended to this affidavit and incorporated herein by reference.

7. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, knowledge obtained from other individuals, including other law enforcement personnel, review of records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this



affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, this affidavit does not set forth each and every fact learned by me during the course of this investigation.

I. BACKGROUND ON DRUG-RELATED MATTERS

8. In a substantial number of residential search warrants executed in connection with the drug investigations in which I and fellow HSI Agents, U.S. Postal Inspectors, Pennsylvania State Police, and other law enforcement officers have been involved, the following kinds of drug-related evidence have typically been recovered from the residences of drug-traffickers:

- a. Controlled substances, such as marijuana, heroin, fentanyl, cocaine, illicit pharmaceuticals, and related precursor chemicals;
- b. Paraphernalia for manufacturing, packaging, processing, diluting, weighing, and distributing controlled substances, such as: pill presses, encapsulating machines, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, microwave ovens, heat-sealing devices, and diluents;
- c. Books, records, receipts, notes, ledgers, invoices, shipping labels, and other papers relating to the importation distribution of controlled substances;
- d. Personal books and papers reflecting names, addresses, telephone numbers, and other contact or identification data relating to the distribution of controlled substances;
- e. Cash, currency, and records relating to controlled substances income and expenditures of money and wealth, for example: money orders, wire transfers (Western Union), cashier's checks and receipts, bank statements, passbooks,

checkbooks, and check registers, as well as precious metals such as gold and silver, and precious gems such as diamonds;

- f. Documents indicating interstate and foreign travel such as travel itineraries, plane tickets, boarding passes, motel and hotel receipts, passports and visas, credit card receipts, telephone bills, and rental car agreements;
- g. Mobile electronic communication devices, such as cellular telephones and “smart phones”, electronic messaging equipment, such as tablets, pagers, telephones, answering machines and their tapes, electronic storage devices, such as GPS devices and portable media players, and other such mobile electronic devices that store data, as well as the content therein;
- h. Firearms and other dangerous weapons; and
- i. Photographs, in particular, photographs of co-conspirators, assets, and/or drugs.

9. In addition, during the course of such residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in the residence, as well as the occupancy, control, or ownership of the subject premises. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, utility and telephone bills, statements, identification documents, and keys to safe deposit boxes and storage facilities.

10. Based upon my training and experience, as well as the knowledge and experience of other agents and police officers involved in this investigation, I am aware that it is generally a common practice for drug traffickers to store their drug inventory and drug-related paraphernalia (as described above) in their residences. Further, it is generally a common practice for drug traffickers to maintain in their residences records relating to their drug trafficking activities.

Because drug traffickers in many instances will “front” (that is, sell on consignment) controlled substances to their clients, or alternatively, will be “fronted” controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed. Such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep “pay and owe” records to show balances due for drugs sold in the past (“pay”) and for payments expected (“owe”) as to the trafficker’s supplier and the trafficker’s dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers and keep them readily available in order to efficiently conduct their drug trafficking business.

11. Based upon my training and experience, I am also aware that it is a generally common practice for traffickers to conceal at their residences large sums of money which represents the proceeds of drug sales or money to be used to purchase additional controlled substances. The large amounts of U.S. currency are necessary to maintain and finance their ongoing drug distribution business. In this connection and context, drug traffickers typically make use of wire transfers, cashier’s checks, and money orders to pay for controlled substances. Evidence of such financial transactions and records relating to income and expenditures of money and wealth in connection with drug trafficking would also typically be maintained in residences.

12. Based upon my training and experience, drug traffickers commonly have in their possession that is, on their person or at their residence, firearms and other dangerous weapons to protect their profits, supply of drugs, and themselves from others who might attempt to forcibly take the traffickers’ profits and/or supply of drugs.

13. Further, I am aware that drug traffickers maintain books, records, receipts, notes, ledgers, bank records, money orders, wire transfer receipts, and other papers relating to the



transportation, ordering, sale, and distribution of controlled substances. Furthermore, I know that the aforementioned books, records, receipts, notes, ledgers, etc. are generally maintained where the traffickers have easy and ready access to them, including in their residences and automobiles.

14. Further, I am aware that persons involved in drug trafficking conceal in their residences and automobiles, currency, financial instruments, precious metals, jewelry, and other items of value and/or proceeds of drug transactions, as well as evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money derived from drug trafficking activities.

15. When drug traffickers amass proceeds from the sale of drugs, they often attempt to legitimize these profits or otherwise conceal them from discovery by law enforcement officers. To accomplish these goals, drug traffickers often use different techniques, including but not limited to: foreign and domestic banks and their attendant services; securities; cashier's checks; money drafts; letters of credit; brokerage houses; the purchase of real estate; as well as shell corporations and business fronts to conceal the true ownership and illegal source of the proceeds.

16. Further, I am aware drug traffickers commonly maintain books or papers that reflect names, addresses, and/or telephone numbers of their associates in the trafficking organization. Also, drug traffickers take or cause to be taken photographs of them, their associates, their property, and their product, and these photographs are usually maintained in their possession.

17. Further, I am aware drug traffickers usually keep paraphernalia for manufacturing, packaging, cutting, weighing, and distributing drugs at their residence. These items are necessary for the drug trafficker to carry on their drug distribution operation.

18. Further, I am aware that drug traffickers often operate under assumed names, street names, or nicknames in order to conceal their true identities from law enforcement officers, and

in so doing, acquire property, services, and personal identification (such as driver's licenses and birth certificates) under their assumed or alias names. Also, they maintain documents of their false identities in their residences and automobiles, together with evidence of their true identities.

19. I have knowledge that drug traffickers commonly conceal their activities from members of the public by transacting their business in a covert manner and frequently conducting their business during the nighttime hours when darkness helps conceal their activities.

20. I have knowledge that it is common for drug dealers to secret contraband, proceeds of drug sales, and records of drug transactions in secure locations within their residence for their ready access and to conceal them from law enforcement authorities.

21. My awareness of these drug trafficking practices, as well as my knowledge of drug use and distribution techniques as set forth in this affidavit, arise from the following:

- a. My own involvement in this and prior drug investigations and searches during my career as a law enforcement officer, as previously described;
- b. My involvement on a number of occasions in debriefing confidential informants and cooperating individuals in prior drug investigations, as well as what other agents and police officers have advised me when relating the substance of their similar debriefings and the results of their own drug investigations; and
- c. Discussion with other federal, state and local law enforcement officers, both about the facts of this case in particular and about trafficking in general.

## II. PROBABLE CAUSE

22. On June 19, 2020, HSI Pittsburgh received information from HSI JFK that on June 18, 2020, they had seized a parcel intended for 715 Clear Ridge Road, Artemas, PA 17211, hereinafter considered the **TARGET PARCEL**. Customs and Border Protection at JFK Airport were conducting an



“enforcement examination of mail shipped from Netherlands, [and] K9 Bence #160608 alerted to this package. The bulky envelope was examined and found to contain a tan rock-like substance secreted within a plastic pouch.” Field tests were conducted and revealed that the substance field tested positive for MDMA/Ecstasy, and weighed approximately 61 grams. The parcel was addressed to “Riggs Viser” and bore multiple stamps instead of a tracking number.

23. Your Affiant conducted a search of Department of Homeland Security (DHS) databases and learned that there was a previous seizure on April 18, 2020, of 112 grams of MDMA/ecstasy, addressed to Riggs Visser, at the **TARGET ADDRESS**. Further, this shipment looked very similar to the **TARGET PARCEL**.

24. Your Affiant conducted a search of the database Clear, which has proven reliable in past investigations. Your Affiant found that a Riggs Visser is currently listed as an occupant at the address of 715 Clear Ridge Road, Artemas, PA 17211. VISSER is shown to be 21 years old. It appears as though the **TARGET PARCEL** is addressed very similarly to VISSER’s real name: Viser, and the single i could be an error on the shipper’s part or it could be a slight difference at the buyer’s request in a small attempt to insulate himself from law enforcement detection. Further, Clear shows several other people using the **TARGET ADDRESS**, where it would appear to be a male and female, most likely VISSER’s parents, and possibly another sibling.

25. Further, a search of the Pennsylvania Justice Network site revealed that Riggs VISSER has a Pennsylvania Driver’s License that lists him at the **TARGET ADDRESS** as of 2017.

26. Your Affiant also conducted a search of VISSER’s criminal history. Your Affiant learned that in July 2017, VISSER was convicted of a misdemeanor drug charge.

27. On June 19, 2020, United States Postal Inspection Service (USPIS) Postal Inspector Staci Johnson conducted surveillance of the **TARGET RESIDENCE**. The **TARGET RESIDENCE** is set off the road a considerable distance, but several outbuildings could be observed as well as several vehicles in the driveway, however make and models, as well as registrations, were not clearly visible.

28. PI Johnson also realized that this was the same shipper as a recent controlled delivery of MDMA, (to a different address), which also originated from the Netherlands. PI Johnson searched Postal records for recent shipments to the **TARGET RESIDENCE**. There appear to be multiple international shipments shipped to the **TARGET RESIDENCE** in 2019 and 2020. It is unknown to whom these parcels were addressed or what was contained within them, however there was one parcel that investigators could identify that also originated from the Netherlands in March 2020. This was the country from where both seizures to VISSER originated.

29. The **TARGET PARCEL** and the other parcels mentioned above, have actually been large envelopes with multiple stamps. Because the **TARGET RESIDENCE** is nearly impossible to sit on and observe the parcel go into the residence from the street, it is necessary to install a GPS tracking device and an electronic beeper to alert investigators if and when the parcel is opened. Also, because this **TARGET PARCEL** is so small, investigators will need to use a different shipping box for the delivery that will allow for the installation of these devices. Accordingly, a larger box will be substituted for the **TARGET PARCEL** and the labels and stamps from the original envelope will be affixed to the shipping box.

COMPUTERS, CELLULAR TELEPHONES, IE: SMART PHONES, and  
ELECTRONIC STORAGE, FOR FORENSIC ANALYSIS

29. As described above and in Attachment B, this application seeks permission to search for records that might be found in the Target Location, in whatever form they are found. One form in which I have probable cause to believe the evidence will be found, is electronically stored on computer hard drives or other storage media, including cellular telephones. Thus, the warrant applied for would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, under Rule 41(e)(2)(B), for later search, and the seizure of certain items within the storage media.

30. *Probable cause.* In my experience, international drug trafficking like at issue in this case, is done through the internet using computers and cellular telephones. The purchases are typically made through illicit websites located outside of the Country and are paid for through Bitcoin, international wire transfer, or some other means requiring the use of the internet. Given the pattern of shipments in this case, I have probable cause to believe that the shipment and payments were arranged through electronic means and that, therefore, there is probable cause to believe that there are computers, cellular telephones, or other electronic media located within the Target Location. I further submit there is probable cause to believe that within the computers, cellular telephones, or other electronic media found within the Target Location will contain evidence of drug trafficking, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.



Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in this application, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause

to believe that this forensic electronic evidence will be on any storage medium in the Target Location because:

- e. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution”

evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For



example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

- j. I know that when an individual uses a computer to obtain drug related items, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

32. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a location for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the location, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- k. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the location could be unreasonable. As explained above, because the warrant calls for forensic electronic

evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- l. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the location. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- m. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.



34. Because several people may share the Target Location as a residence, it is possible that the Target Location will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this application could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

### III. CONCLUSION

35. Your Affiant along with additional law enforcement personnel will attempt a controlled delivery of the **TARGET PARCEL** to the **TARGET RESIDENCE**. If the **TARGET PARCEL** is accepted at the **TARGET RESIDENCE**, Your Affiant is requesting that an anticipatory search warrant for the residence be granted.


36. The Triggering Event for execution of the anticipatory search warrant will be that the **TARGET PARCEL** is accepted at the **TARGET RESIDENCE**. Upon occurrence of the triggering event, Your Affiant believes that within the **TARGET RESIDENCE**, will be the items described in Attachment B.

37. Additionally, Your Affiant respectfully requests an order authorizing the installation and real-time monitoring of an electronic alerting device “beeper” and a GPS tracking device. Both devices will be secreted within the Suspect Parcel prior to the attempted controlled delivery and will be continuously monitored until said Suspect Parcel and contents are secured by law enforcement personnel involved in this operation.

The above information is true and correct to the best of my knowledge, information and belief.

/s/ Brianna M. Tetrault  
Brianna M. Tetrault  
Special Agent  
Homeland Security Investigations

Sworn and subscribed before me, by telephone  
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),  
this 22<sup>nd</sup> day of June, 2020.

  
\_\_\_\_\_  
KEITH A. PESTO  
United States Magistrate Judge